REMARKS

1-2. 35 U.S.C. § 112. Rejections.

2. Claims 1-30 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Office Action states that "the terms "public key" identifier and "private key" in claims 1 and 16 are used by the claim to mean an identifying number (e.g. an account number) while the accepted meaning is "a code used to encrypt a 'message' such that a private key (also a code) is needed to decrypt that 'message'. Applicant is respectfully requested to change those terms used throughout the specification and claims to a term more in keeping with Applicant's intended meaning.

Applicant has amended the Application, Figure 3, Figure 4, Figure 7, Figure 8, Figure 9, and Figure 12, and Claims 1-3, 6-8, 10-17, 21-23, and 26-30, to claim the disclosed "public key" as a --public identifier--, to claim the disclosed "supplementary public key" as a --supplementary public identifier--, and claim the disclosed "private key" as a --private identifier--.

Support for the use of a public identifier, supplementary public identifier, and private identifier is seen in the Application as filed, at least on page 7, lines 6-26; on page 13, line 6 to page 15, line 16; on page 19, lines 13-24; on page 21, line 33 to page 22, line 25; on page 25, lines 12-18; on page 30, lines 21-27; in Figure 4 (element 100); in Figure 5 (element 128); and in Figure 12 (element 80,82).

The Office Action also states that "in Claim 2, line 4, there is no proper antecedent basis for "authorization module". Perhaps the term "authorization" should be changed to –authentication--.

Applicant has amended dependent Claim 2 to claim that the defined virtual certificate "further comprises a second public identifier defined by said issuer user, wherein said second public identifier is stored at said certificate authority, and wherein said authentication module requires a submittal of said second public identifier, and a matching comparison to said second public identifier stored at said certificate authority."

Support is seen in the Application as filed, at least on page 11, lines 19-20; on page 13, lines 10-12; on page 14, lines 11-18; on page 14, line 31 to page 15, line 16; on page 19, lines 13-20; on page 23, lines 26-28; on page 27, lines 9-19.

Applicant therefore respectfully submits that Claims 1-3, 6-8,10-17, 21-23, and 26-30, as amended, overcome the rejections under 35 U.S.C. §112, second paragraph. As Claims 4, 5, and 9 depend from amended independent Claim 1, and as Claims 18-20, 24, and 25 depend from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

3-4. 35 U.S.C. § 102. Rejections.

4. Claims 1-9, 15-24 and 30 are rejected under 35 U.S.C. §102(e) as being anticipated by Tedesco et al (U.S. Patent No. 2002/0062286 A1).

Applicant has amended independent Claim 1, to claim that the certificate authority is "adapted to allow the definition of a virtual certificate comprising a redemption denomination and a first public identifier, wherein said redemption denomination corresponds to any of a product, a service, a coupon, and a reservation, said redemption denomination defined b y an issuer user in communication with said certificate authority across said network, said issuer user associated with a redemption location, and wherein said first public identifier is defined by said certificate authority".

Applicant has also amended independent Claim 16, to claim the step of "defining a virtual certificate on a certificate authority, said defined virtual certificate comprising a redemption denomination and a first public identifier, wherein said redemption denomination corresponds to any of a product, a service, a coupon, and a reservation, said redemption denomination defined by an issuer user in communication with said certificate authority across said transaction network, said issuer user associated with a redemption location, and wherein said first public identifier is defined by said certificate authority".

Support is seen in the Application as filed, as least on page 9, lines 10-30; on page 10, line 15 to page 11, line 23; on page 16, line 11 to page 18, line 11; on page 28, line 29 to page 29, line 29; on page 40, lines 6-31; on page 42, lines 19-27; in Figure 1; in Figure 5; in Figure 9 to Figure 11; and in Figure 14 to Figure 16.

A description of the creation of virtual certificates is seen in the Application as filed, at least on page 9, lines 12-21, wherein;

> "one or more virtual certificates 60 are remotely created, such as by an issuer user ISR (FIG. 9), through issuer facilities 24 (*e.g.* such as through a web portal interface). The virtual certificates 60 typically correspond to a sellable commodity, such as a product or service denomination, which is selectable by the issuer user ISR. In an alternate embodiment, the virtual certificates 60 may correspond to a distributable commodity, such as a discount coupon for a product or service, or a reservation (*e.g.* such as for travel or dining), which is selectable by the issuer user ISR."

A description of an issuer user and the creation of one or more customized virtual certificates is seen in the Application as filed, at least on page 10, line 20 to page 11, line 8, wherein;

> "An issuer user ISR 22 at an issuer terminal 22, in selective electronic communication with a certificate authority 12, has the means (*i.e.* issuer facilities) 24 to direct the certificate authority 12 to create one or more customized virtual certificates 60, for subsequent issuance to acquirer users ACQ at one or more acquirer terminals 26.
>
> **Establishment of Defined Virtual Certificates.** Authorization for the construction of certificates typically occurs through an issuer facility 24, such as through a web portal 24 for a transaction network 10 operating across an internet 192, whereby an issuer user ISR (*e.g.* such as a merchant, or a product manager for a plurality of stores RL) connects to the certificate authority 12 (*i.e.* such as through a certificate server portion 14 of a certificate authority 12).
>
> The issuer user ISR defines detailed specifications for virtual single-use certificates 60 through a certificate specification interface 194 (FIG. 10), such as design specifications 62 and redemption rules 66, whereby the certificates 60 typically reflect sellable or distributable commodities, such as products and/or services which are available for pick up by a customer, typically at a redemption location RL (*e.g.* such as at a retail store, a distribution center, a box office, a ticket counter, or at a service provider)."

Further details regarding the creation of virtual certificates by an issuer user is seen in the Application as filed, at least on page 28, lines 29-33, wherein;

> "Figure 9 shows the creation of a virtual certificate 60 by an issuer user ISR at an issuer terminal 22, through issuer facilities 24. As described above, an issuer user ISR, in communication with the certificate authority 12 across a network 192 (*e.g.* such as the internet), typically through a certificate server 14, can direct the creation of one or more virtual certificates 60."

Details regarding the advantages of the creation of virtual certificates is seen in the Application as filed, at least on page 42, lines 19-27, wherein;

> "Retailers, such as small merchants or service providers, may easily establish means for selling their goods and services online, without the requirement of establishing an extensive online presence. Issuers may simply register their business with the certificate authority 12, and then may create virtual certificates 60 for one or more of their products and services. Virtual certificates 60 can be offered for acquisition at one or more network sites, such as an aggregated site 234 for a large variety of products and services within a selected region, or a more specialized site 234 that is related to specific types of products or services within their area."

An overview of the method and apparatus for processing checks to reserve funds, as described by Tedesco et al, is seen at least in the Abstract, wherein:

> "A bank device communicates with an account holder device, such as a telephone or computer operated by the account holder. The bank device receives therefrom check data that includes an account identifier, a check identifier, and an amount of funds. The account identifier indicates a financial account and the check identifier indicates a check drawn on the financial account. The amount of funds represents an amount to reserve for payment with the check. The bank device in tum makes the amount of funds unavailable for use in the financial account so the account holder may not withdraw or otherwise remove the amount of funds. The bank device generates a code that indicates the check, and transmits the code to the account holder device. Subsequently, a payee, such as a merchant presented with the specified check, may verify that the check does indeed have an amount of funds reserved for payment therewith. The bank device receives the code from the payee, and determines the amount of funds that are reserved for payment with the check. An

appropriate message that indicates the reserved amount of funds is transmitted to the payee."

Applicant respectfully submits that, while Tedesco et al describes a method and apparatus for processing checks to reserve funds, there is no disclosure in Tedesco et al of a virtual certificate comprising a redemption denomination which corresponds to any of a product, a service, a coupon, and a reservation, which is defined by an issuer user in communication with a certificate authority across a transaction network, in which the issuer user associated with a redemption location.

Applicant therefore respectfully submits that the method and apparatus for processing checks to reserve funds described by Tedesco et al is significantly different than the present invention, as claimed in Claim 1 and Claim 16, as amended.

As seen in Tedesco et al, at least in the Abstract, a "A bank device communicates with an account holder device, such as a telephone or computer operated by the account holder. The bank device receives therefrom check data that includes an account identifier, a check identifier, and an amount of funds."

Applicant respectfully submits that, while a bank device receives check data from a telephone or computer operated by the account holder, there is no disclosure that the check data comprises a redemption denomination which corresponds to any of a product, a service, a coupon, and a reservation, which is defined by an issuer user in communication with a certificate authority across a transaction network, in which the issuer user associated with a redemption location, as claimed in Claim 1 and Claim 16, as amended.

Therefore, Applicant submits that Claim 1 and Claim 16, as amended, overcome the rejections under 35 U.S.C. §102(e) as being anticipated by Tedesco et al (U.S. Patent No. 2002/0062286 A1). As dependent claims 2-9 and 15 depend from amended independent Claim 1, and as dependent claims 17-24 and 30 depend from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

5-6. 35 U.S.C. § 103. Rejections.

6. Claims 10-14 and 25-29 are rejected under 35 U.S.C. §103(a) as being unpatentable over Tedesco et al (U.S. Patent No. 6,000,832) in view of Walker et al (U.S. Patent No. 6,193,155).

Applicant has amended independent Claim 1, to claim that the certificate authority is "adapted to allow the definition of a virtual certificate comprising a redemption denomination and a first public identifier, wherein said redemption denomination corresponds to any of a product, a service, a coupon, and a reservation, said redemption denomination defined by an issuer user in communication with said certificate authority across said network, said issuer user associated with a redemption location, and wherein said first public identifier is defined by said certificate authority".

Applicant has also amended independent Claim 16, to claim the step of "defining a virtual certificate on a certificate authority, said defined virtual certificate comprising a redemption denomination and a first public identifier, wherein said redemption denomination corresponds to any of a product, a service, a coupon, and a reservation, said redemption denomination defined by an issuer user in communication with said certificate authority across said transaction network, said issuer user associated with a redemption location, and wherein said first public identifier is defined by said certificate authority".

Support is seen in the Application as filed, as least on page 9, lines 10-30; on page 10, line 15 to page 11, line 23; on page 16, line 11 to page 18, line 11; on page 28, line 29 to page 29, line 29; on page 40, lines 6-31; on page 42, lines 19-27; in Figure 1; in Figure 5; in Figure 9 to Figure 11; and in Figure 14 to Figure 16.

An overview of the method and apparatus for issuing and managing gift certificates, as described by Walker et al, is seen at least in the Abstract, wherein:

> "The present invention relates to a method and apparatus for issuing and redeeming a gift certificate drawn on a credit card or other financial account. The present invention includes a first aspect directed to a merchant card authorization terminal and a second aspect directed to a credit card issuer central controller. According to the first aspect, a method for redeeming a gift certificate drawn on a financial account is disclosed including the steps of receiving a gift certificate for payment of an identified value, transmitting a request for authorization to a central server, receiving an authorization signal, representing an indication that redemption of the gift certificate is authorized,

from said central server and receiving a payment from the account issuer based on said identified value. A system is also disclosed for implementing the methods in all aspects of the present invention. "

Details regarding a gift certificate in Walker et al are seen at least in col. 5, lines 8-12, wherein:

> "a gift certificate may be any instrument or token which represents financial value, including a traditional paper certificate, a stored value card, or a magnetic stripe card having an alias account number thereon."

As seen in a first embodiment of Walker et al, at least on col. 5, lines 38, a "credit card holder 104 determines a maximum value for the certificate and transfers the certificate, including the certificate identifier and an indication of the maximum value, to recipient 106. Recipient 106 may then present the gift certificate to pay for goods and/or services at participating merchants, such as merchant 108. A participating merchant is one that is capable of processing credit card transactions on behalf of the credit card issuer designated on the gift certificate".

Further details of gift certificates of Walker et al seen at least in Figure 8 and on col. 8, lines 55-64, wherein:

> "Gift certificate 800 is a single-use financial instrument that may be negotiated by the bearer, as indicated by the example at reference numeral 810. Gift certificate 800 corresponds to record 502 of certificate table 500, and includes the name of the credit card holder 812, a maximum value 814, and an expiration date 816. Gift certificate 800 expires on Jan. 15, 1997 and is redeemable for merchandise worth up to the maximum value, in this case $50.00. Alternatively, gift certificate 800 may be redeemed for $50.00 cash."

Applicant therefore respectfully submits that while Walker et al describe an method and apparatus for issuing and managing gift certificates, Walker et al do not disclose or suggest a virtual certificate comprising a redemption denomination which corresponds to any of a product, a service, a coupon, and a reservation, which is defined by an issuer user in communication with a certificate authority across a transaction network, in which the issuer user associated with a redemption location.

Therefore, Applicant respectfully submits that neither Tedesco et al nor Walker et al, alone or combined, disclose or suggest a virtual certificate comprising a redemption denomination which corresponds to any of a product, a service, a coupon, and a reservation, which is defined by an issuer user in communication with a certificate authority across a network, in which the issuer user associated with a redemption location. It would therefore take significant modification and undue experimentation to meet Claim 1 and Claim 16, as amended.

Therefore, Applicant submits that Claim 1 and Claim 16, as amended, overcome the rejections under 35 U.S.C. §103(a) as being unpatentable over Tedesco et al (U.S. Patent No. 6,000,832) in view of Walker et al (U.S. Patent No. 6,193,155). As dependent claims 10-14 depend from amended independent Claim 1, and as dependent claims 25-30 depend from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

7. Applicant has amended dependent Claim 2, to provide proper antecedent terminology for the claimed invention. Applicant has also amended dependent Claim 3, to correct a grammatical error. Applicant has also amended the Specification, to indicate the claim for priority to U.S Provisional Application No. 60/113,706, filed 24 December 1998. Applicant has also amended the Specification, to provide corrections to reference characters. Applicant has also amended Figure 3, Figure 9, and Figure 12, to correct spelling and grammatical errors.

CONCLUSION

Applicant therefore respectfully submits that Claims 1-30, as amended, overcome the rejections set forth in the Office Action. Applicant also submits that the amendments do not introduce new matter into the Application. Based on the foregoing, Applicant considers the invention to be in condition for allowance. Applicant earnestly solicits the Examiner's withdrawal of the rejections set forth in the prior Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent.

Respectfully Submitted,

Michael A. Glenn
Reg. No. 30,176

Customer No. 22862

Please amend the Application as follows:

Marked-up Version to Show Changes in the Specification

On Page 1, line 5 of the Application, please insert the following section:

CLAIM FOR PRIORITY

This application claims priority of U.S Provisional Application No. 60/113,706, filed 24 December 1998.

On Page 7, lines 6-26 of the Application, please replace the paragraph with the following paragraph, as amended:

A transaction network contains a networked certificate authority, by which one or more virtual certificates may be remotely defined and stored, such as by an issuer user through a issuer web portal interface. The virtual certificates correspond to a product or service denomination which is selected by the issuer, include a public ~~key~~ identifier. An acquirer user may locate and acquire one or more virtual certificates, through an acquirer web portal interface. When a virtual certificate is acquired by an acquirer, a corresponding private ~~key~~ identifier is established by the acquirer, and is stored at the certificate authority in association with a record of the acquired certificate. As well, when the certificate is acquired, the acquirer typically submits payment agent information (*e.g.* such as credit card information). In one embodiment, funds are transferred during acquisition of the certificate. In a preferred embodiment, authorization for the transfer of funds occurs during the acquisition transaction. Certificate information is typically transferred to the acquirer, or to an alternate recipient, by which the holder of the certificate can redeem the certificate at a redemption location associated with an acquired certificate. The acquirer (or an alternate recipient of an acquired certificate to whom the acquirer has communicated the established private ~~key~~ identifier), submits the certificate information at the redemption location, along with the established private ~~key~~ identifier, to redeem the certificate. Upon communication of valid certificate information to the certificate authority, the redemption of the acquired certificate is authorized, while further use of the certificate is revoked.

On Page 8, lines 4-5 of the Application, please replace the phrase with the following phrase, as amended:

Figure 4 shows a redemption process for a single-use gift certificate having an identification packet and an associated private ~~key~~ identifier;

On Page 9, line 23 to page 10, line 12 of the Application, please replace the paragraphs with the following paragraphs, as amended:

An acquirer user ACQ (FIG. 6), accessing the transaction network 10 through an acquirer terminal 26, may locate and acquire one or more virtual certificates 60, through an acquirer facilities 28 (*e.g.* such as through an acquirer web portal interface). When a virtual certificate 60 is acquired by an acquirer user ACQ, a corresponding private ~~key~~ identifier 76 is established, either by the acquirer user ACQ, or by the certificate authority 12, and is stored at the certificate authority 12 (*e.g.* such as within the database 18), in association with a record of the acquired certificate 60, along with other identifying information 98 for the acquired certificate 60.

As well, when a virtual certificate 60 is acquired, the acquirer user ACQ typically submits payment agent information 52 (*e.g.* such as credit card information). In one embodiment, funds are transferred during acquisition of the certificate 60. In a preferred embodiment, authorization for the subsequent transfer of funds occurs during the acquisition transaction 72. Certificate information 98 (FIG. 3) is typically transferred to the acquirer user ACQ, or to an alternate recipient RCP, by which the holder of the acquired certificate 60 can redeem the certificate 60 at a redemption location RL (FIG. 4,8) associated with an acquired certificate 60. The acquirer ACQ (or an alternate recipient RCP of an acquired certificate 60 to whom the acquirer user ACQ has communicated the established private ~~key~~ identifier 76), submits the certificate information at the redemption location RL, along with the established private ~~key~~ identifier 76, to redeem the certificate. Upon communication of valid certificate information to the certificate authority 12, the redemption of the acquired certificate 60 is authorized, while further use of the acquired certificate 60 is revoked.

On Page 11, lines 9-23 of the Application, please replace the paragraph with the following paragraph, as amended:

An issuer user ISR 22 has the means 122 (FIG. 5) to control the modular design of one or more virtual certificates 60a-60n independently, either by selecting standard designs offered by the certificate authority 12, by uploading 122 one or more custom designs 62a-

62n to the certificate authority 12, in the form of a computer file, or by specifying that a certificate 60 be issued using a combination of stock elements 162 uploaded through the issuer terminal 22. An issuer user may preferably incorporate the denomination 64 (*i.e.* a redemption value) of the certificate 60 as an additional element in the certificate identification packet 74. The denomination 64 typically corresponds to a product or service, or a selectable quantity of goods or services, which is to be received upon redemption of an acquired certificate 60. Additionally, an issuer user ISR may preferably incorporate an additional public ~~key~~ identifier segment 82, as a part of the certificate identification packet 74, which may be used, for example, in mapping a certificate 60 to an issuer's coding scheme (*e.g.* such as to correspond to product serial numbers, part numbers, product color codes, product size, or service codes).

On Page 12, lines 5-10 of the Application, please replace the paragraph with the following paragraph, as amended:

Acquisition of Certificates and Establishment of ~~Keys~~ Identifiers. Figure 3 is a schematic view of an acquisition transaction 72 for a single-use certificate 60. identification packet 74. During an acquisition transaction 72, an acquirer user ACQ typically provides a means to purchase a certificate 60, an authorization to purchase during a subsequent redemption transaction 104 (FIG. 4), or otherwise qualifies for issuance of the acquired certificate 60.

On Page 13, line 6 to page 15, line 30 of the Application, please replace the paragraphs with the following paragraphs, as amended:

During an acquisition transaction 72, in which the certificate authority 12 issues a certificate 60 to the acquirer user ACQ, a unique identifier 98 is bound to the issued certificate 60, typically comprising certificate information 74, which appears on the acquired certificate 60, which typically includes a denomination 64, and a public ~~key~~ identifier 80 assigned by the certificate authority 12. In a preferred embodiment, the certificate information 74 includes a supplementary public ~~key~~ identifier segment 82, which is assigned by an issuer user ISR. The certificate information 74 typically appears on the acquired certificate 60 through a printed number 68, or through other indicia, such as an encoded symbol, bar code, or three-dimensional bar code 70 (FIG. 2). Certificate information 74 which appears as human-readable information 68 or machine-readable information 70 on a printed acquired certificate 60 is preferably tamper-resistant. The unique certificate identifier 98 includes the elements associated with the certificate information 74, in combination with a private ~~key~~ identifier 76, which is assigned to the certificate 60 as a part of the acquisition transaction 72.

The private ~~key~~ identifier 76 is assigned to the certificate 60 at the time of acquisition, typically either by the acquirer user 92 or by the certificate authority 12. In embodiments in which the private ~~key~~ identifier 76 is assigned to an acquired certificate 60 by the certificate authority 12, the private ~~key~~ identifier 76 is typically generated randomly by the certificate authority 12, or is generated to comply with identification parameters selected 128 (FIG. 5) by an issuer user ISR. In embodiments in which the private ~~key~~ identifier 76 is assigned to an acquired certificate 60 by the acquirer user ACQ, the private ~~key~~ identifier 76 may be a unique private ~~key~~ identifier 76 input by the acquirer user ACQ at he time of acquisition, or may alternately be a private ~~key~~ identifier 76 which is used for one or more acquired certificates 60 for the acquirer user ACQ (*e.g.* such as a reusable "purchase PIN", or the acquirer's facility 28 access PIN).

The established private ~~key~~ identifier 76 does not appear on the certificate 60, and is known only to the acquirer user ACQ, but is stored by the certificate authority 12, in association with the other data elements relating to the certificate 60, on the secure database 18.

Redemption of Certificates. Figure 4 shows a redemption process 90 for a single-use gift certificate 60 having a submitted identification packet 98, which includes and an associated private ~~key~~ identifier 76. The private ~~key~~ identifier 76 must be provided to the redeemer 36 as part of the redemption process 90 by the acquirer user ACQ (FIG. 4), or by a third party and/or agent RCP to whom the acquirer ACQ has communicated the private ~~key~~ identifier 76. A redemption clerk RC, such as a sales clerk, through a redeemer terminal 36, in communication with the certificate authority 12, by means of the redeemer facilities 38, or optionally, by means of a live operator intermediary 42, may authenticate a certificate 60, by providing the certificate authority 12 with the unique identification information 98 associated with the acquired certificate 60 (*i.e.* both the public ~~keys~~ identifiers 80,82 assigned to the certificate upon issuance, a denomination 64, as well as the unique private identification information 76 which is assigned to the certificate 60 upon acquisition (*i.e.* the private ~~key~~ identifier 76).

In alternate embodiments of the certificate system 10, either the redemption clerk RC or the holder of the acquired certificate 60 can manually or automatically upload the certificate information ~~76~~ 72 during a redemption process 90, such as through a point of sale terminal 40. As well, either the redemption clerk RC or the holder of the acquired certificate 60 can enter the private ~~key~~ identifier PIN 76 into a point of sale terminal 40. One or more redeemer terminals 36, point of sale terminals 40, and/or telephonic devices 40 may be located at the redemption location RL, and may include a variety wireless network communications, such as a localized wireless network at the redemption location RL, or as remote wireless connections across a network 192 (FIG. 9) to the certificate authority 12.

Authorization of Certificate During Redemption. The certificate authority 12 authenticates a certificate 60, on the basis of the certificate identification packet 74 (which includes the public ~~key~~ identifier 80 and supplementary public ~~key~~ identifier 82), and the private ~~key~~ identifier 76 submitted by a redemption clerk RC, such as through redemption terminal 36 (or alternately, by the holder ACQ,RCP of the certificate 60, such as directly into a point of sale terminal 40). As seen in comparison step 100 in Figure 4, the certificate authority 12 queries the secure database 18, which stores the independent elements associated with the acquired certificate 60, to determine whether the certificate identification packet 74 and the private ~~key~~ identifier 76 originally associated with the certificate 60 upon issuance matches the certificate identification packet 74 and private ~~key~~ identifier 76 identification information provided to the certificate authority 12 through the redeemer facilities 38, as shown in matching step 102. If the unique identification sets correlate 103, the certificate authority 12 validates the certificate 60, and upon instructions by the redemption clerk RC, authorizes the redemption transaction 104. If the unique identification sets do not correlate 105, the certificate authority 12 typically cancels 106 the redemption transaction 104, either by requesting that the acquirer ACQ resubmit the certificate information 74 and the private ~~key~~ identifier 76, or by revoking the certificate 60 (*e.g.* such as if the certificate 60 has previously been marked as used).

Authorized Redemption Transaction and Cancellation of Single-Use Certificate. Upon a successful authorization transaction 104 of an acquired certificate 60, the certificate authority 12 allows the redemption clerk RC to proceed with redemption of the certificate 60, and revokes the single-use certificate 60 (*i.e.* thus preventing further use of the certificate information 74,76). The certificate authority 12 revokes the acquired certificate 60 by updating the certificate information stored on the secure database 18 (*e.g.* by marking the acquired certificate as "used"). In one embodiment of the certificate system 10, the certificate authority 12, by means of certificate payment facilities 48, initiates the transfer of payments between the parties of the acquisition transaction ~~76~~ 72 and the redemption transaction 104, by issuing transfer instructions to the certificate payment agent 58, the acquirer payment agent 52, the issuer payment agent 54, and the redeemer payment agent 56.

On Page 19, lines 13-24 of the Application, please replace the paragraph with the following paragraph, as amended:

At issuance certificate identification parameter selection step 128, the issuer preferably selects or specifies the format of unique certificate supplementary public ~~key~~ identification 82 (FIGS. 3,4). For example, the issuer may require unique certificate public ~~key~~ identification 82 which corresponds to existing product codes, inventory, or existing issuer certificate systems. Therefore, the issuer may optionally select, enter or upload certificate identification supplementary public ~~key~~ identifier parameters 82, to be combined with certificate identification public ~~key~~ identifier information 80 (FIG. 3) assigned by the certificate authority 12. As well, in a preferred embodiment of the certificate identification parameter selection step 128, the issuer user ISR may select the format used by the certificate authority ~~76~~ 12 to establish private ~~keys~~ identifiers 76, or to guide the input of private ~~keys~~ identifiers 76 by an acquirer user ACQ, during an acquisition transaction 72.

On Page 21, line 24 to page 22, line 29 of the Application, please replace the paragraphs with the following paragraphs, as amended:

Certificate Acquisition and Input of Acquirer Information. Figure 7 shows a detailed acquisition transaction process 150, by which an acquirer user may direct a certificate authority 12 to issue one or more selected certificates 60a 60n from an inventory of available virtual certificates 60. An acquirer typically receives an issued certificate 60, in exchange for an authorization to charge the acquirer upon certificate redemption, for payment at the time of acquisition, or on the basis of other acquirer qualifications. An acquirer may upload other necessary instructions and transaction information 162 to the certificate authority 12, which are then stored (*e.g.* such as in database 18) as additional independent elements associated with the issued certificate 60. Acquirer entered transaction information 162 typically includes name and address information 164, credit card or other information 166 associated with the acquirer's payment agent 52, assignment 170 by the acquirer of the secret private ~~key~~ identifier 76 (FIG. 3) to be associated with the selected certificate 60, and a selected delivery method 172 for the certificate 60. As described above, the private ~~key~~ identifier 76 is established in relation with an acquired certificate 60 at the time a certificate 60 is acquired, whereby the private ~~key~~ identifier 76 is established by the certificate authority 12, or is entered by the acquirer user ACQ.

For a private ~~key~~ identifier 76 which is established by the acquirer user ACQ, the private ~~key~~ identifier 76 may be unique to a single transaction 72. As well, the acquirer user ACQ may alternately establish a private "acquisition" ~~key~~ identifier 76, which may be associated with one or more acquisition transactions 72. Furthermore, the acquirer user ACQ may alternately use the established acquirer registration ~~key~~ identifier 142 as a private ~~key~~ identifier 76, which is then associated with one or more acquisition transactions 72.

The acquirer is typically prompted (*e.g.* such as by a required data entry field or a dialog box) to input the private ~~key~~ identifier 76 (*e.g.* such as a personal identification number (PIN) into the system. The acquirer is preferably prompted to enter the private ~~key~~ identifier 76 twice, to verify that the acquirer user has correctly entered a known private ~~key~~ identifier), to be stored in association with the certificate 60. In a preferred embodiment of the certificate system 10, an acquirer may specify that the private ~~key~~ identifier 76 to be associated with an issued certificate 60 be comprised of other identification information associated with the transaction, such as an account number which associates the acquirer with the acquirer's payment agent 52 (*e.g.* a credit card number), or a debit card number. As well, an acquirer user ACQ may preferably select and/or specify a denomination 168 for an acquired certificate 60 (*e.g.* such as a currency amount), typically by selecting from among denominations presented by an issuer. In a preferred embodiment of the certificate system 10, the certificate authority 12 sends a confirming e-mail to the acquirer.

On Page 23, lines 8-16 of the Application, please replace the paragraph with the following paragraph, as amended:

The acquirer user ACQ can preferably send an e-mail or other message to an alternate recipient RCP (*e.g.* such as for a gift certificate), directing the recipient RCP to log on and pick up the certificate, either for printing, such as at the recipient's computer, at the redemption location RL, or at a third party (*e.g.* such as at a third party mail service provider). If no hard-copy of the acquired certificate 60 is desired, or if printing is not feasible, the certificate information can be transferred directly to the issuer merchant's computer (*e.g.* a paperless electronic certificate), by which the acquirer ACQ or alternate recipient RCP need only to visit a redemption location RL, and supply the private ~~key~~ identifier PIN number 76 to the redemption clerk RC.

On Page 23, lines 26-32 of the Application, please replace the paragraph with the following paragraph, as amended:

A redeemer (*i.e.* a store clerk) typically needs only the certificate information 74 (which includes the denomination 78 of the certificate 60 and public ~~keys~~ identifiers 80,82), in combination with the acquirer's private ~~key~~ identifier 76, to validate an acquired certificate 60. Hence, an issuer may request that a certificate 60 be delivered in the form of an e-mail, containing only these items, or as encodeable "smart card" data that can be magnetically stored by the acquirer using a "smart card" encoder 34 attached to the acquirer computer 26 or other communication device.

On Page 24, lines 13-26 of the Application, please replace the paragraphs with the following paragraphs, as amended:

As seen in Figure 6, until an acquired certificate is redeemed, an acquirer preferably has the ability to cancel 152 a previously acquired certificate 60, or to request that an acquired certificate be revoked and replaced 153 by a new certificate 60. For example, if an acquirer user accidentally damages, destroys, or loses a previously printed acquired certificate 60, the acquirer may simply print out a new certificate 60, or have a new certificate delivered or faxed, and may either retain the previously stored private ~~key~~ identifier 76, or may specify a new private ~~key~~ identifier 76.

Since an acquired certificate 60 may only be used for redemption once (at which time further use is revoked), there is no financial risk to the issuer ISR in the use of replacement certificates 60, or that a downloaded certificate 60 be printed more than once. As well, even if a certificate is lost and retrieved by a second party, or is stolen, the lost acquired certificate is unredeemable, without submittal of the private ~~key~~ identifier 76, which is not included as printed information on a certificate 60.

On Page 25, lines 13-18 of the Application, please replace the paragraph with the following paragraph, as amended:

In addition to the previously defined public ~~keys~~ identifiers 80,82 and private ~~key~~ identifiers, upon issuance of an acquired certificate, the certificate authority 12 preferably creates or assigns a unique issued certificate number (*e.g.* such as certificate "XYZ-203-4067") which corresponds to the acquired certificate 60, as well as to the collection of the defined elements of the certificate 60 (*e.g.* such as the associated graphics 62, redemption rules 66, and denomination 78), which are bound within the database 18 after the acquisition transaction.

On Page 27, lines 1-23 of the Application, please replace the paragraphs with the following paragraphs, as amended:

When an acquirer user ACQ (or alternate recipient RCP) desires to proceed with a redemption transaction 90 at a redemption location, the acquirer user ACQ typically hands the printed certificate 60 to a redemption clerk RC, and communicates the private ~~key~~ identifier 76. The redemption clerk RC then validates the issued certificate 60, to obtain a redemption authorization code 181 from a certificate authority 12 to redeem the certificate 60, thereby performing a certificate authentication 178. In a preferred embodiment of the certificate system, the acquired certificate includes redemption instructions 66 (*i.e.* terms of service instructions), which a redemption clerk RC preferably follows to redeem the acquired certificate 60. The redemption clerk RC uploads 180 certificate information 98 to the certificate authority 12, which typically includes the certificate denomination 78, the public ~~keys~~ identifiers 80,82, as well as the private ~~key~~ identifier 76 (which is submitted separately by the acquirer user ACQ).

In a preferred embodiment of the certificate system 10, communication of redemption information 98 (*e.g.* such as communication of the required public ~~keys~~ identifiers 80,82, private ~~key~~ identifier 76 and denomination 78) of the certificate 60 to the certificate authority 12 is made by an electronic link 39 with a point-of-sale (POS) terminal 40 and/or a card code scanner 40, a redeemer computer 36, or by other means having the ability to establish an electronic link 39 with the certificate authority 12. For example, a redemption clerk RC preferably uses a bar code image scanner or other POS terminal 40 to determine the redemption information 98, while the acquirer ACQ typically enters the private ~~key~~ identifier 76 (*e.g.* such as a PIN number) into a keypad of a POS terminal 40.

On Page 27, line 31 to page 28, line 3 of the Application, please replace the paragraph with the following paragraph, as amended:

Authorization of Certificate Redemption. Upon authentication of the certificate by the certificate authority 12, on the basis of a correlation of the unique certificate identification 74 in combination with the acquirer's private ~~key~~ identifier PIN 76 with the transaction records associated with the certificate 60 stored in the secure database 18, the certificate authority 12 authorizes the redemption, and revokes further use of the acquired certificate 60.

On Page 28, line 29 to page 29, line 4 of the Application, please replace the paragraph with the following paragraph, as amended:

Issuer Creation Module. Figure 9 shows the creation of a virtual certificate 60 by an issuer user ISR at an issuer terminal 22, through issuer facilities 24. As described above, an issuer user ISR, in communication with the certificate authority 12 across a network 192 (*e.g.* such as the internet), typically through a certificate server 14, can direct the creation of one or more virtual certificates 60. The issuer facilities preferably include a issuer certificate creation module 194, in which the issuer may define attributes for a virtual certificate 60, such as denomination information 64a,64b, certificate design information 62a-62n, redemption rules 66a-66n, and issuer defined supplementary public ~~key~~ identifier information 82.

On Page 30, lines 21-27 of the Application, please replace the paragraph with the following paragraph, as amended:

Creation of Inventory. Figure 12 is a block diagram 226 of a virtual inventory 228 stored within a database 18. Each created virtual certificate 60 is a defined collection of elements, such as denomination elements 64a,64b, redemption rules 66, such as applicable redemption locations RL, and a public ~~key~~ identification packet 80,82. One or more virtual certificates 60, which are stored within the database 18, become a virtual inventory 228 of goods and services, which can then be accessed through one or more network locations (*e.g.* such as through web sites).

On Page 35, lines 1-8 of the Application, please replace the paragraph with the following paragraph, as amended:

As described above, during an acquisition transaction 72, the acquirer facilities 28 typically prompt the acquirer user ACQ to enter required transaction information 150 (FIG. 5), and manages the establishment of the private ~~key~~ identifier 76, which is thereafter associated with the acquired certificate 60. As described above, the private ~~key~~ identifier 76 may be submitted by the acquirer ACQ during the acquisition transaction 72, or may alternately be communicated to the acquirer ACQ from the certificate authority 12 during the acquisition transaction 72.

On Page 37, line 28 to page 38, line 5 of the Application, please replace the paragraph with the following paragraph, as amended:

In the preferred certificate system 10 wherein payment is not transferred until actual redemption of the certificate 60, buyers are inherently protected from mis-represented goods or services, or from illegitimate certificate issuers ISR. If a customer, such as an acquirer user, or a recipient of a certificate 60 (and accompanying private ~~key~~ identifier 76), decides not to redeem the certificate, or upon visiting a redemption location RL, decides against the transaction for any reason, the customer may, at their discretion, decide against proceeding with the redemption transaction 104. Since the customer is not charged for the sale unless a redemption transaction 104 is actually made, the customer is inherently protected, since the certificate system 10 minimizes misrepresentation of goods and services by issuers ISR.

On Page 39, line 29 to page 40, line 4 of the Application, please replace the paragraph with the following paragraph, as amended:

However, within the certificate system 10, for embodiments where funds are initially locked during the acquisition, and where a second authorization takes place upon redemption of an acquired certificate, funds are transferred at the redemption level. For an acquirer user ACQ who has a card present for redemption authorization, there is a reasonable level of security for the merchant that the card is valid. Even for an acquirer ACQ or recipient RCP who is in possession of the certificate 60 and the private ~~key~~ identifier 76, the redemption transaction is significantly more secure than a remote internet transaction. Therefore, a merchant is more likely to pay less to the credit card issuing agency.

On Page 41, lines 1-18 of the Application, please replace the paragraphs with the following paragraphs, as amended:

System Applications and Alternative Embodiments. The certificate system 10 can be used for a large variety of commerce applications, wherein products and services are located on-line, but are picked up at a store RL. For example, an acquirer user ACQ may locate a large gift item on-line (*e.g.* such as a television set), which can be picked up at a location RL near a recipient RCP. The acquirer user ACQ may simply search for and locate the desired gift item at a location RL near the recipient RCP, proceed with an acquisition transaction 72, transfer the acquired certificate 60 (or just the certificate information 74) to the recipient RCP (or directly to the redemption location RL), and communicate the private ~~key~~ identifier to the recipient RCP. The recipient RCP may then perform the redemption transaction 90, and receive the gift item.

In a similar embodiment, an acquirer user ACQ may desire to send a gift certificate with a selected money denomination 64 to a recipient RCP. With the certificate information 74 and the private ~~key~~ identifier 76, the recipient RCP can either visit the redemption location RL directly, or may alternately browse on-line through an aggregate site 234 or a merchant site 242, to locate desired goods or services, before picking the desired goods up at the redemption location RL.

On Page 41, line 32 to page 42, line 11 of the Application, please replace the paragraph with the following paragraph, as amended:

As described above, the certificate system 10 does not require that monetary funds are transferred, or that the system be used exclusively for purchasing products or services. For example, the certificate system 10 may be used to distribute discount coupons for one or more issuers ISR, which are typically redeemable as a discount for an acquired product or service. While virtual coupons are similar to virtual certificates 60, there is typically no monetary value associated with a virtual coupon, such that there may be no private ~~key~~ identifier verification required during a redemption transaction 90. An acquirer user ACQ simply accesses a desired virtual coupon (*e.g.* such as for a related search for products or businesses within their regional area), and prints a desired coupon on an acquirer printer 30. The acquirer user ACQ may then visit a related redemption location RL (*i.e.* the selected store), which honors and redeems the coupon (typically as a discount for a product or service specified on the virtual coupon).

Status of the Claims

1. (Currently Amended) A certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption denomination and a first public identifier, wherein said redemption denomination corresponds to any of a product, a service, a coupon, and a reservation, said redemption denomination defined by an issuer user in communication with said certificate authority across said network, said issuer user associated with a redemption location, and ~~a~~ wherein said first public ~~key~~ identifier is defined by said certificate authority;

a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate comprising said redemption denomination and said first public ~~key~~ identifier, said creation of said issued certificate associated with a private ~~key~~ identifier which is assigned at time of said acquisition of said virtual certificate, wherein said private ~~key~~ identifier does not appear on said issued certificate, and wherein said redemption denomination, said first public ~~key~~ identifier, and said assigned private ~~key~~ identifier are stored at said certificate authority in association with said issued certificate;

a certificate authentication module for authorization of an off-line redemption of said issued certificate at ~~a~~ said redemption location to a holder of said issued certificate located at said redemption location, said holder comprising any of said acquirer user and an alternate recipient of said issued certificate to whom said acquirer user has communicated said private ~~key~~ identifier, said authorization based upon a communication from said redemption location to said certificate authority of said redemption denomination and said first public ~~key~~ identifier from said issued certificate, a communication of said private ~~key~~ identifier provided by said holder, and a matching comparison of said redemption denomination, said first public ~~key~~ identifier, and said private ~~key~~ identifier stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said certificate authority.

2. (Currently Amended) The certificate system of Claim 1, wherein said defined virtual certificate ~~includes~~ further comprises a second public ~~key~~ identifier defined by said issuer user, wherein said second public ~~key~~ identifier is stored at said certificate authority, and wherein said ~~authorization~~ authentication module requires a submittal of said second public ~~key~~ identifier, and a matching comparison to said second public ~~key~~ identifier stored at said certificate authority.

3. (Currently Amended) The certificate system of Claim 1, wherein said ~~a~~ certificate issuance module requires the submittal of a payment agent by said acquirer user.

4. (Previously Amended) The certificate system of Claim 3, wherein said required submittal of said payment agent for said acquirer user comprises an authorization to transfer funds from said payment agent for said acquirer upon creation of said issued certificate.

5. (Previously Amended) The certificate system of Claim 3, wherein said required submittal of said payment agent for said acquirer user comprises an authorization to transfer funds from said payment agent for said acquirer upon redemption of said issued certificate.

6. (Currently Amended) The certificate system of Claim 1, wherein said certificate issuance module comprises means to deliver said redemption denomination, said first public ~~key~~ identifier, and said assigned private ~~key~~ identifier to said acquirer user.

7. (Currently Amended) The certificate system of Claim 6, wherein said means to deliver said redemption denomination and said first public ~~key~~ identifier to said acquirer user comprises a printed form of said issued certificate.

8. (Currently Amended) The certificate system of Claim 6, wherein said means to deliver said redemption denomination and said first ~~public~~ key identifier to said acquirer user comprises an electronic form of said issued certificate.

9. (Original) The certificate system of Claim 1, wherein said holder of said issued certificate is said acquirer user.

10. (Currently Amended) The certificate system of Claim 1, wherein said holder of said issued certificate is said alternate recipient who submits said private ~~key~~ identifier.

11. (Currently Amended) The certificate system of Claim 1, wherein said assigned private ~~key~~ identifier is entered by said acquirer user during said selectable acquisition of said virtual certificate.

12. (Currently Amended) The certificate system of Claim 11, wherein said entered, assigned private ~~key~~ identifier is uniquely associated with a single acquired issued certificate.

13. (Currently Amended) The certificate system of Claim 11, wherein said entered, assigned private ~~key~~ identifier is a private purchase ~~key~~ identifier unique to said acquirer user.

14. (Currently Amended) The certificate system of Claim 11, wherein said entered, assigned private ~~key~~ identifier is a private acquirer facility access ~~key~~ identifier unique to said acquirer user.

15. (Currently Amended) The certificate system of Claim 1, wherein said assigned private ~~key~~ identifier is established by said certificate authority during said selectable acquisition of said virtual certificate.

16. (Currently Amended) A process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual certificate ~~comprised of~~ comprising a redemption denomination and a first public identifier, wherein said redemption denomination corresponds to any of a product, a service, a coupon, and a reservation, said redemption denomination defined by an issuer user in communication with said certificate authority across said transaction network, said issuer user associated with a redemption location, and ~~a~~ wherein said first public ~~key~~ identifier is defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate comprising said redemption denomination and said first public ~~key~~ identifier, said creation of said issued certificate associated with an establishment of a private ~~key~~ identifier which does not appear on said issued certificate, said redemption denomination, said first public ~~key~~ identifier, and said established private ~~key~~ identifier stored at said certificate authority in association with said issued certificate;

authorizing an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate, said holder comprising any of said acquirer user and an alternate recipient of said issued certificate to whom said acquirer user has communicated said private ~~key~~ identifier, wherein said authorization is based upon redemption submittal at said redemption location of said redemption denomination and said first public ~~key~~ identifier from said issued certificate, a communication of said private ~~key~~ identifier provided by said holder, and a matching comparison of said redemption denomination, said first public ~~key~~ identifier, and said private ~~key~~ identifier stored at said certificate authority; and canceling further redemption of said issued certificate at said certificate authority.

17. (Currently Amended) The process of Claim 16, wherein said step of defining said virtual certificate, wherein said defined virtual certificate comprises a second public ~~key~~ identifier defined by said issuer user, wherein said step of creating said issued certificate includes the storage of said second public ~~key~~ identifier at said certificate authority, and wherein said step of authorizing said redemption of said issued certificate comprises a submittal of said second public ~~key~~ identifier, and a matching comparison to said second public ~~key~~ identifier stored at said certificate authority.

18. (Previously Amended) The process of Claim 16, wherein said step of creation of said issued certificate comprises the submittal of a payment agent by said acquirer user.

19. (Previously Amended) The process of Claim 18, wherein said submittal of said payment agent for said acquirer user comprises an authorization to transfer funds from said payment agent for said acquirer during said step of creation of said issued certificate.

20. (Previously Amended) The process of Claim 18, wherein said submittal of said payment agent for said acquirer user comprises an authorization to transfer funds from said payment agent for said acquirer during said step of redemption of said issued certificate.

21. (Currently Amended) The process of Claim 16, wherein said step of creation of said issued certificate comprises a delivery of said redemption denomination and said first public ~~key~~ identifier to said acquirer user.

22. (Currently Amended) The process of Claim 21, wherein said delivered redemption denomination and said first public ~~key~~ identifier are included in a printed form of said issued certificate.

23. (Currently Amended) The process of Claim 21, wherein said delivered redemption denomination and said first public ~~key~~ identifier are included in an electronic form of said issued certificate.

24. (Original) The process of Claim 16, wherein within said authorizing step, said holder of said issued certificate is said acquirer user.

25. (Previously Amended) The process of Claim 16, wherein within said authorizing step, said holder of said issued certificate is said alternate recipient.

26. (Currently Amended) The process of Claim 16, wherein said established private ~~key~~ identifier is entered by said acquirer user.

27. (Currently Amended) The process of Claim 26, wherein said entered established private ~~key~~ identifier is uniquely associated with a single acquired issued certificate.

28. (Currently Amended) The process of Claim 26, wherein said entered established private ~~key~~ identifier is a private purchase ~~key~~ identifier that is unique to said acquirer user.

29. (Currently Amended) The process of Claim 26, wherein said entered established private ~~key~~ identifier is a private acquirer facility access ~~key~~ identifier that is unique to said acquirer user.

30. (Currently Amended) The process of Claim 16, wherein said established private ~~key~~ identifier is established by said certificate authority and communicated to said acquirer.

Amendments to the Figures

In Figure 3, please replace "Key" with --Identifier-- within element (76), as shown in amended formal Figure 3.

In Figure 3, please replace "Key" with --Identifier-- within element (80), as shown in amended formal Figure 3.

In Figure 3, please replace "Key" with --Identifier-- within element (82), as shown in amended formal Figure 3.

In Figure 3, please insert ")" after "Assigned by Issuer" within element (82), as shown in amended formal Figure 3.

In Figure 4, please replace "Key" with --Identifier-- within element (96), as shown in amended formal Figure 4.

In Figure 7, please replace “Key” with --Identifier--within element (170), as shown in amended formal Figure 7.

In Figure 8, please replace “Public Key and Private Key” with --Public Identifier and Private Identifier-- within element (180), as shown in amended formal Figure 8.

In Figure 9, please replace “Key” with --Identifier-- within element (82), as shown in amended formal Figure 9.

In Figure 9, please replace “Smothie” with --Smoothie-- within element (64b), as shown in amended formal Figure 9.

In Figure 12, please replace “Public Key ID Packet” with --Public ID Packet-- associated with element (80,82), as shown in amended formal Figure 12.

In Figure 12, please replace “Vitual Certificates” with --Virtual Certificates-- associated with element (228), as shown in amended formal Figure 12.